

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-059355

(43)Date of publication of application : 25.02.2000

(51)Int.Cl. H04L 9/16  
G06F 13/00  
G09C 1/00  
H04L 9/18  
H04L 9/36

(21)Application number : 10-220198

(71)Applicant : DAINIPPON PRINTING CO LTD

(22)Date of filing : 04.08.1998

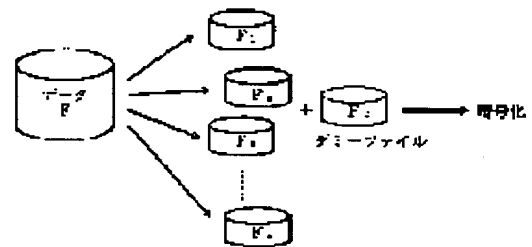
(72)Inventor : YANO YOSHIHIRO  
MATSUDA MASAYUKI  
HANDA TOMIO  
SHIBATA NAOTO

## (54) ENCIPHERING PROCESSING SYSTEM

### (57)Abstract:

PROBLEM TO BE SOLVED: To improve security by enhancing secrecy as an entire file by diving transmission data into plural parts and enciphering them through are or plural enciphering systems while using one or plural cryptographic keys.

SOLUTION: An enciphering device sets the length of a divided file, enciphering system, formula for finding the cryptographic key and respective initial values. Original data F are divided into F1, F2,..., Fn by a dividing means, and the order of divided files is rearranged as needed. When they are rearranged, indexes showing dividing positions are added and slave files are recognized. After a dummy file FD is as needed, the entire file is enciphered by one enciphering system and cryptographic key or enciphered by changing the enciphering system and cryptographic key for each divided file, and then outputted. A deciphering device deletes the indexes showing the order or dividing positions and repeatedly deciphers each slave file while using respective conditions at the time of enciphering. When completed, the files are merged again so that the original transmission data are obtained.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-59355

(P2000-59355A)

(43)公開日 平成12年2月25日(2000.2.25)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	ターミナル*(参考)
H 0 4 L 9/16		H 0 4 L 9/00	6 4 3 5 B 0 8 9
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 E 5 K 0 1 3
G 0 9 C 1/00	6 1 0	G 0 9 C 1/00	6 1 0 A
	6 6 0		6 6 0 D
H 0 4 L 9/18		H 0 4 L 9/00	6 5 1

審査請求 未請求 請求項の数 3 O L (全 4 頁) 最終頁に続く

(21)出願番号 特願平10-220198

(22)出願日 平成10年8月4日(1998.8.4)

(71)出願人 000002897

大日本印刷株式会社

東京都新宿区市谷加賀町一丁目1番1号

(72)発明者 矢野義博

東京都新宿区市谷加賀町一丁目1番1号大

日本印刷株式会社内

(72)発明者 松田雅之

東京都新宿区市谷加賀町一丁目1番1号大

日本印刷株式会社内

(74)代理人 100092495

弁理士 蛭川 昌信 (外7名)

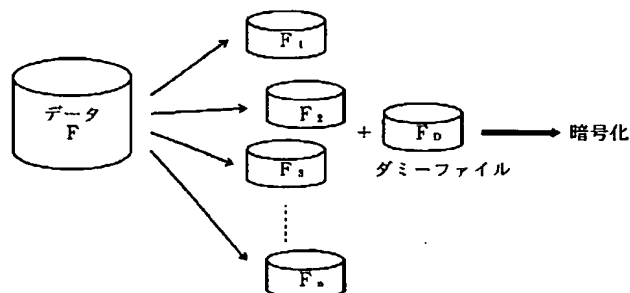
最終頁に続く

(54)【発明の名称】 暗号化処理システム

(57)【要約】

【課題】 ファイル全体としての隠蔽性を高くし、高い安全性を保つことができるようにする。

【解決手段】 送信データを複数の分割する分割手段と、分割手段により分割したデータの一部または全部を暗号化する暗号化手段と、暗号化手段により暗号化したデータを送信する送信手段とを備えたことを特徴とする。



## 【特許請求の範囲】

【請求項1】 送信データを複数に分割する分割手段と、分割手段により分割したデータの一部または全部を暗号化する暗号化手段と、暗号化手段により暗号化したデータを送信する送信手段とを備えた暗号化処理システム。

【請求項2】 前記分割したデータの暗号化は、1つあるいは複数の暗号化方式により、1つあるいは複数の暗号鍵を用いて暗号化することを特徴とする請求項1記載の暗号化処理システム。

【請求項3】 前記分割したデータに、さらにダミーデータを付加することを特徴とする請求項1または2記載の暗号化処理システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は送信データを暗号化し、通信回線を通して受信側にデータを伝送する暗号化処理システムに関するものである。

## 【0002】

【従来の技術】一般に、任意のファイルについて暗号化を行う場合、当該ファイルに対して1つの暗号鍵を用い、1つの暗号方法により一括して暗号化が施される。また、第3者による暗号文への攻撃に対応するため、暗号化された文をさらに分割し、分割したデータを、順次、回線上に分配し、回線上を伝送されてくる分配されたデータを再び元の順番に並べ変える手法も提案されている（特開平3-108830号公報）。

## 【0003】

【発明が解決しようとする課題】何らかの暗号解読方法、例えば既知の平文攻撃（電子メール等の場合、書き出し部分には定型的な文章が多く現れることを利用し、攻撃者にとって既知の平文と暗号文の対を基に共通鍵を導き出す攻撃）により、ファイルの一部について暗号が破られた場合、ファイルの全体についても同様の手法で暗号が破られる危険性がある。また、特開平3-108830号公報で提案されているように、暗号化してからファイルを分割した場合、これを第3者が解読することは困難にはなるが、ファイルの一部の解読が全体に波及することには変わらない。本発明は上記課題を解決するためのもので、ファイル全体としての隠蔽性を高くし、高い安全性を保つことができるようにすることを目的とする。

## 【0004】

【課題を解決するための手段】本発明は、送信データを複数に分割する分割手段と、分割手段により分割したデータの一部または全部を暗号化する暗号化手段と、暗号化手段により暗号化したデータを送信する送信手段とを備えたことを特徴とする。また、本発明は、前記分割したデータの暗号化は、1つ或いは複数の暗号化方式により、1つ或いは複数の暗号鍵を用いて暗号化することを

特徴とする。また、本発明は、前記分割したデータに、さらにダミーデータを付加することを特徴とする。

## 【0005】

【発明の実施の形態】以下、本発明の実施の形態について説明する。図1は本発明の暗号化処理システムの全体図である。送信側は送信端末装置1と暗号化装置2からなり、送信端末装置1は暗号化装置2を介して、暗号化した送信データを通信回線5に送出する。受信側は復号装置3、受信端末装置4からなり、暗号化されたデータを受信端末装置4で受信して復号装置3で復号する。

【0006】図2は本発明の暗号化装置2の機能を示すブロック図である。暗号化装置2には送信するデータファイルを分割するファイル分割手段21、必要に応じてダミーファイルを付加するダミーファイル付加手段22、分割ファイルを並び替える並び替え手段23、分割したファイルを個々に暗号化する分割ファイル暗号化手段24を備えている。

【0007】ファイル分割手段21は、例えば分割するための数式を1つまたは複数有していて、使用する数式をランダムに決定し、初期値を任意に設定して数式よりファイルの分割位置を決定する方式、あるいは乱数を発生させ、これを利用してファイルの分割位置を決定する方式等、適宜の方式を用いる。分割した各ファイルには、その分割位置を示す指標を付したり、あるいは分割位置を示すテーブルを作成する。

【0008】ダミーファイル付加手段22は、一定数、一定サイズのダミーファイルを生成して付加したり、ファイル分割数に応じて付加するダミーファイルの数やそのサイズを変えて付加するものであり、ダミーファイルには、そのこと示す何らかの情報、例えば指標を付加する。

【0009】並び替え手段23は、乱数を発生させてファイルを並べる順番を決めたり、或いは1つまたは複数の数式をもっておき、任意に初期値を設定すること等により順番を決定する。

【0010】分割ファイル暗号化手段24は、複数の暗号化方式、暗号鍵を有していて、分割ファイル全体を1つの暗号化方式、暗号鍵で暗号化したり、各分割ファイル毎、或いはいくつかのファイル毎に暗号化方式、暗号鍵を変えて暗号化を行う。また、暗号化はファイルの一部に行ってもよい。

【0011】図3に模式的に示すように、暗号化装置2のファイル分割手段21により元のデータFは複数のファイル $F_1$ 、 $F_2$ …… $F_n$ に分割され、ダミーファイル付加手段22により、必要に応じてダミーファイル $F_D$ が付加され、並び替え手段23により必要に応じて並び替えが行われ、分割ファイル暗号化手段24により暗号化されて送信される。ファイルの並び替えは暗号化の前であっても、後であってもよく、また、ファイルの分割と並び替え、暗号化は並列的に処理を行ってもよい。

【0012】図4は復号装置3の機能ブロック図である。受信した各分割ファイルを復号する分割ファイル復号手段31と、復号した手段を再統合するファイル統合手段32とを備えている。分割ファイル復号手段31には、送信側での各ファイルごとの暗号化方法、暗号鍵等の情報、暗号化を行ったファイルか否か等の情報があらかじめ設定される。ファイル統合手段32には、ファイル単位の分割の仕方、ファイル単位の分割位置の情報を知らなければならない、そのため、例えば分割のための数式だけを決めておき、送信側から初期値を設定すると、受信側ではその初期値を基に順次分割位置を計算によって求めるようにする等の方法が採用可能である。また、ファイル分割方法、各分割ファイルの暗号化方法、暗号鍵等をICカードに格納しておき、これを送信側、受信側に配布するようにしてもよい。このようなICカードを利用すれば、回線上に暗号化に関する情報が流れないので、一層秘密性を保持することができる。

【0013】次に、図5により暗号化／復号処理フローの例を説明する。暗号化処理を説明すると、図5(a)において、まず、用いる暗号の方式、分割して細分化するファイルの長さを求める数式とこれの初期値、細分化されたファイルを暗号化する方式を決定する数式とこれの初期値、それぞれの暗号化に用いる鍵を求める数式とその初期値を設定する(S1)。次いで、与えられたファイルを規則に従って分割し(S2)、これに暗号化を施す(S3)。分割された個々のファイル(以下、子ファイル)についてはその順番を維持するか、何らかの規則に従って並び替えを行う。並び替えた場合、それらの順番や最終子ファイルを表わす指標を付加する(S4)。子ファイルは外部から個々のファイルとして認識されるか、あるいは全体が1つのファイルとして認識される。子ファイルに指標を付けず、これらを管理し、最

後の子ファイルを認識するためのテーブルを用意しておいても良い。こうしてファイルが最後か、否か判断し(S5)、最後になるまで以上の処理を繰り返す。

【0014】次に、復号処理を説明すると、図5(b)において、まず、順番や最終子ファイルを表わす指標を削除し(S11)、暗号化した時のそれぞれの条件を用いて個々の子ファイルの復号を行い(S12)、その結果を出力し(S13)、この処理を最後まで繰り返し(S14)、最後まで復号処理したらファイルを再統合する(S15)。

【0015】

【発明の効果】以上のように、本発明によれば、ファイル全体としての隠蔽性が高くなるため、高い安全性を保つことができる。また、暗号手法の強度、例えば暗号鍵の長さ等に関して、何らかの制限があり、十分安全な暗号方式を使用できない場合にもファイル全体として高い安全性を保つことが可能となる。

【図面の簡単な説明】

【図1】 本発明の暗号化処理システムの全体図である。

【図2】 本発明の暗号化装置2の機能を示すブロック図である。

【図3】 ファイル分割を模式的に示す図である。

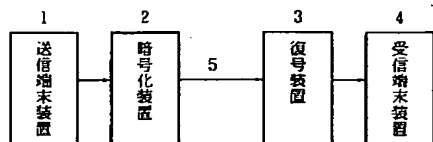
【図4】 復号装置の機能ブロック図である。

【図5】 暗号化／復号処理フローの例を説明する図である。

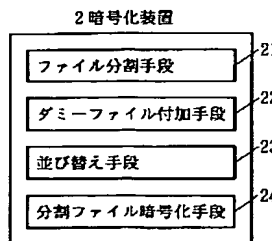
【符号の説明】

1…送信端末装置、2…暗号化装置、3…復号装置、4…受信端末装置、5…通信回線、21…ファイル分割手段、22…ダミーファイル付加手段、23…並び替え手段、24…分割ファイル暗号化手段、31…分割ファイル復号手段、32…ファイル統合手段。

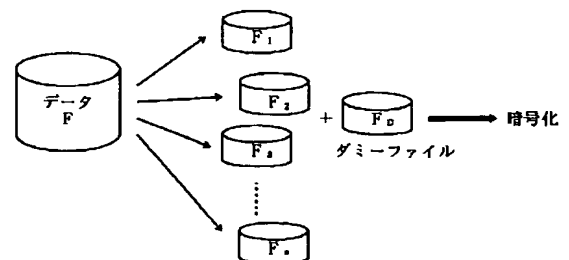
【図1】



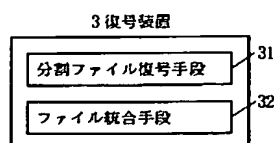
【図2】



【図3】



【図4】



【図5】



フロントページの続き

(51) Int. Cl. 7

H04L 9/36

識別記号

F I

H04L 9/00

テ-マ-ド (参考)

6 8 5

(72) 発明者 半田富己男

東京都新宿区市谷加賀町一丁目1番1号大  
日本印刷株式会社内

(72) 発明者 柴田直人

東京都新宿区市谷加賀町一丁目1番1号大  
日本印刷株式会社内

Fターム (参考) 5B089 KA17 KC57 KH30  
5K013 BA03 FA02 FA05